#11

BRIEF ON APPEAL

Thomas Spinelli
Attorney for Appellant
Registration No. 39,533

SCULLY SCOTT MURPHY & PRESSER
400 Garden City Plaza
Garden City, New York 11530
(516) 742-4343

TABLE OF CONTENTS

		PAGE
I.	INTRODUCTION	1
II.	REAL PARTY OF INTEREST	1
III.	RELATED APPEALS AND INTERFERENCES	2
IV.	STATUS OF THE CLAIMS	2
V.	STATUS OF THE AMENDMENTS	6
VI.	SUMMARY OF THE INVENTION	7
VII.	THE APPEALED CLAIMS	8
VIII.	THE PRIOR ART RELIED UPON	15
IX.	THE ISSUES	15
X.	THE REFERENCES	16
XI.	GROUPING OF THE CLAIMS	16
XII.	APPELLANTS' ARGUMENTS	17
	A. The rejection of Claims 1-3, 5-16, 18-26, 33-37, 47-49, 51-62, 64-72, 79-83, 117-121, 124-128, and 130-133 on appeal under 35 U.S.C. § 103(a) as being allegedly unpatentable over U.S. Patent No. 5,646,997 to Barton (hereinafter "Barton") in view of Applied Cryptography by Schneier (hereinafter "Schneier") is improper	17
	B. The rejection of Claims 27-32 and 73-78 on appeal under 35 U.S.C. § 103(a) as being allegedly unpatentable over Barton in view of Schneier and further in view of U.S. Patent No. 5,579,393 to Conner (hereinafter "Conner") is improper	24
	C. The rejection of Claims 38-41, 84-87, 106-116, 122, 123, 129, and 134 on appeal under 35 U.S.C. § 103(a) as being allegedly unpatentable over Barton in view of Schneier and further in view of U.S. Patent No. 5,771,101 to Bramall (hereinafter "Bramall") is improper	24
XIII.	CONCLUSION	26
	APPENDIX	28

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicant:	Ingemar J. Cox, et al.	**Examiner:**	A. DiLorenzo
Serial No.:	09/294,956	**Art Unit:**	2766
Filed:	April 20, 1999	**Docket:**	12558 (SGNA1014)
For:	METHOD AND DEVICE FOR INSERTING AND AUTHENTICATING A DIGITAL SIGNATURE IN DIGITAL DATA	**Dated:**	March 12, 2001

Hon. Commissioner of Patents
and Trademarks
Washington, DC 20231

BRIEF ON APPEAL

Sir:

I. INTRODUCTION

Pursuant to the provisions of 35 U.S.C. § 134 and 37 C.F.R. §§ 1.191 and 1.192, this paper is submitted as a brief setting forth the authorities and arguments upon which Appellants rely in support of the appeal from the Final Rejection of Claims 1-3, 5-16, 18-41, 47-49, 51-62, 64-87, and 108-134 in the above-identified patent application on August 14, 2000.

II. REAL PARTY OF INTEREST

The real party of interest in the above-identified patent application is NEC Corporation.

III. RELATED APPEALS AND INTERFERENCES

Appellants respectfully submit that the present application is involved in no other appeal or interference besides the present Appeal.

IV. STATUS OF THE CLAIMS

The present application, U.S. patent application Serial No. 09/294,956 filed on April 20, 1999, originally included Claims 1-116.

In an Official Action dated February 11, 2000, the Examiner rejected claims 1, 3, 4, 47, 49, 50, 94, and 98 under 35 U.S.C. § 102(b) as being anticipated by Barton (5,646,997). Additionally, the Examiner rejected claims 2, 5-17, 22-26, 33-37, 42-45, 48, 51-63, 68-72, 79-83, 88-91, 95-97, 99, and 100-107 under 35 U.S.C. § 103(a) as being unpatentable over Barton and further in view of Schneier (Applied Cryptography). Furthermore, the Examiner rejected claims 27-32, 46, 73-78, 92, and 93 under 35 U.S.C. § 103(a) as being unpatentable over Barton in view of Schneier and further in view of Conner (5,579,393). Lastly, the Examiner rejected 38-41, 84-87, and 108-116 under 35 U.S.C. § 103(a) as being unpatentable over Barton in view of Schneier and further in view of Bramall (5,771,101).

In a Response under 37 C.F.R. § 1.111, filed May 10, 2000, Applicants argued that independent claims 108 and 112 patentably distinguished over the prior art and were allowable.

With regard to claims 17, 22-24, 63, and 68-70, Applicants also argued that there was no teaching or suggestion in the cited references to place a public key, needed to decrypt a digital signature, into associated data.

With regard to claims 26, 72, 95, 96, 99, and 100, Applicants also argued that the cited references did not teach or suggest receiving associated data from an external source such as from a global positioning satellite transmission (claims 26 and 72), from a radio transmission (claims 95 and 99), or via an Internet link (claims 96 and 100).

With regard to claims 36 and 82, Applicants also argued that there was no teaching or suggestion in the cited references of transmitting a hash and signature to a third party over the Internet and receiving a time stamp from the third party over the Internet.

Furthermore, with regard to claims 38, 40, 86, 108, 112, and 114, Applicants also argued that there was no teaching or suggestion in the cited references of recognizing a user of the device whose identifier is stored in memory and inserting the identifier as the associated memory (claim 38 and 108, 112), particularly where the means to recognize the user is a fingerprint recognition means (claims 40, 86, and 114).

Consequently, the claims were amended to emphasize the features of dependent claims 17, 22-24, 26, 36, 38, 40, 63, 68-70, 72, 82, 86, 95, 96, 99, 100, and 114. Specifically:

Claim 1 was amended to include the features of claim 17 and intervening claim 4, claims 4 and 17 were canceled, and those claims depending thereon were amended;

Claim 47 was amended to include the features of claim 63 and intervening claim 50, claims 50 and 63 were canceled, and those claims depending thereon were amended;

New claim 117 was added merging the features of claims 1, 4, and 22, new claims 118 and 119 were also added, claim 118 depended from claim 117 which added the features of claim 23 and new claim 119 depended from claim 118 which added the features of claim 24;

New claim 120 was added merging the features of claims 1, 4, 25, and 26;

New claim 121 was added merging the features of claims 1 and 36 as well as intervening claims 34 and 35;

New claim 122 was added merging the features of claims 1 and 38 as well as intervening claim 4, claim 123 was also added which depended from claim 122 and having the features of claim 40;

New claim 124 was added merging the features of claims 47, 50, and 68, claims 125 and 126 were also added, claim 125 depended from claim 124 and added the features of claim 69, claim 126 depended from claim 125 and added the features of claim 70;

New claim 127 was added merging the features of claims 47 and 72 as well as intervening claims 50, 65, and 71;

New claim 128 was added merging the features of claims 47 and 82 as well as intervening claims 50, 80, and 81;

New claim 129 was added merging the features of claims 47 and 86 as well was intervening claims 50 and 84;

New claim 130 was added merging the features of claims 94 and 95;

New claim 131 was added merging the features of claims 94 and 96;

New claim 132 was added merging the features of claims 98 and 99;

New claim 133 was added merging the features of claims 98 and 100; and

New claim 134 was added merging the features of claims 112 and 114.

In the Final Official Action, issued August 14, 2000, the Examiner maintained the rejections of the claims under 35 U.S.C. § 103(a) and also rejected the claims added in the Response filed on May 10, 2000. Specifically, the Examiner rejected claims 1-3, 5-16, 18-26, 33-37, 47-49, 51-62, 64-72, and 79-83 under 35 U.S.C. § 103(a) as being unpatentable over Barton in view of Schneier. Additionally, the Examiner rejected claims 27-32 and 73-78 under 35 U.S.C. § 103(a) as being unpatentable over Barton in view of Schneier and further in view of Conner. Furthermore, the Examiner rejected claims 38-41, 84-87, and 106-116 under 35 U.S.C. § 103(a) as being unpatentable over Barton in view of Schneier and further in view of Bramall. Lastly, the Examiner rejected the newly added claims in the previous Response. Specifically, the Examiner rejected claims 117-121, 124-128, and 130-133 under 35 U.S.C. § 103(a) as being unpatentable over Barton in view of Schneier and rejected claims 122, 123, 129, and 134 under 35 U.S.C. § 103(a) as being unpatentable over Barton in view of Schneier and further in view of Bramall.

Consequently, Claims 1-3, 5-16, 18-41, 47-49, 51-62, 64-87, and 108-134 are the claims on appeal. A copy of the rejected claims is attached hereto in the Appendix.

In a Response under 37 C.F.R. § 1.116, filed November 22, 2000, Applicants reiterated their previous arguments from the Response filed May 10, 2000, Namely, that:

1. there is no teaching or suggestion in the cited references to place a public key, needed to decrypt the digital signature, into the associated data (claims 17, 22-24, 63, 68-70, 117-119, and 124-126);

2. there is no teaching or suggestion in the cited references to receive associated data from an external source such as from a global positioning satellite transmission (claims 26, 72, 120, and 127), from a radio transmission (claims 95, 99, 130, and 132), or via an Internet link (claims 96, 100, 131, and 133);

3. there is no teaching or suggestion in the cited references of transmitting a hash and signature to a third party over the Internet and receiving a time stamp from the third party over the Internet (claims 36, 82, 121, and 128); and

4. there is no teaching or suggestion in the cited references of recognizing a user of the device whose identifier is stored in memory and inserting the identifier as the associated memory (claim 38, 108, 112, and 122), particularly where the means to recognize the user is a fingerprint recognition means (claims 40, 86, 114, 129, and 134).

Subsequent to the filing of the Response under 37 C.F.R. § 1.116, an Advisory Action was issued on December 4, 2000, indicating that the Response under 37 C.F.R. § 1.116 was considered but that the arguments set forth therein were not persuasive.

V. STATUS OF THE AMENDMENTS

Appellants have not filed any amendments subsequent the issuance of the Final Rejection of November 22, 2000.

VI. SUMMARY OF THE INVENTION

The present invention relates to methods and devices for inserting and authenticating a digital signature and associated data in digital image, video, and audio data.

In the methods and devices of the present invention, a signature is inserted into predetermined bits of digital data for authentication of the digital data. Alternatively, both the digital data and some associated information are both authenticated. This associated information might include copyright notices, owner identification, amongst other things. This information may be embedded into the image in a variety of ways, as have been discussed in the watermarking literature. This embedding is performed prior to signing (creating the digital signature by hashing and encrypting).

In a version of the methods and devices of the present invention, the concern is with the situation in which a compression algorithm is well known to the authentication system. This approach is applicable to, for example a JPEG compressed image or MPEG compressed video. In particular, the present invention is applicable to the problem of authentication within a digital camera or other image generation devices, though the solution is not limited to such a situation. Digital cameras with resolutions of 1Kx1K produce very large amounts of data which must be both stored and possibly transmitted from the camera to a computer. To expedite this process, it is expected that such data will be compressed in order to reduce the storage and bandwidth requirements. However, when the image is eventually decompressed, the viewer must still be able to authenticate the image.

In another version of the methods and devices of the present invention not only is digital data signed for authentication purposes but it is also time stamped in order to be able to prove the time of origin. A further refinement of this system is to time stamp the image with both time and place of the image generation device, the latter information preferably being available through a Global Positioning Satellite (GPS) receiver.

VII. THE APPEALED CLAIMS

Claims 1-3, 5-16, 18-41, 47-49, 51-62, 64-87, and 108-134 are on appeal before the Board of Patent Appeals and Interferences, with Claims 1, 47, 108, 112, 117, 120, 121, 122, 124, and 127-134 being the independent claims.

Independent Claim 1 is directed to a method for inserting a digital signature into digital data, where the digital data comprises bits. The method recited in independent claim 1 assigns predetermined bits of the digital data for receiving the digital signature, inserts associated data into the digital data; signs the digital data (excluding the predetermined bits) which results in the digital signature. The digital signature is then inserted into the predetermined bits of the digital data for subsequent authentication of both the digital data and the associated data. Claim 1 further recites that at least a portion of the associated data comprises data identifying a public key needed to decrypt the digital signature. Claims 2, 3, 5-16, and 18-41 directly or indirectly depend upon Claim 1 and further limit the scope of Claim 1.

Independent claim 47 is directed to an encoder which carries out the method of claim 1 and is similar in scope thereto. Dependent Claims 48, 49, 51-62, and 64-87 directly or indirectly depend upon Claim 47.

Independent claim 108 is directed to a method for inserting data into digital data wherein an identifier corresponding to each of at least one user of a device which creates the digital data is stored; a user of the device whose identifier is stored in a memory is recognized; the identifier corresponding to the recognized user is output from the memory; and data corresponding to the identifier is inserted into the digital data. Dependent Claims 109-116 directly or indirectly depend upon Claim 108.

Independent claim 117 is similar in scope to original claim 1 but adds the features of original claims 4, and 22. That is, independent claim 117 recites a method for inserting a digital signature into digital data where the digital data comprises bits and the method comprises: assigning predetermined bits of the digital data for receiving the digital signature; inserting associated data into the digital data; signing the digital data excluding the predetermined bits resulting in the digital signature; and inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and associated data; wherein the associated data comprises at least two fields. Dependent Claims 118 and 119 directly or indirectly depend upon Claim 117.

Independent claim 120 is similar in scope to original claim 1 but adds the features of original claims 4, 25, and 26. That is, independent claim 120 recites a method for inserting a digital signature into digital data where the digital data comprises bits and the method comprises: assigning predetermined bits of the digital data for receiving the digital

signature; receiving associated data from a Global Positioning Satellite transmission; inserting the associated data into the digital data; signing the digital data excluding the predetermined bits resulting in the digital signature; and inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and associated data.

Independent claim 121 is similar in scope to original claim 1 but adds the features of original claim 36 as well as intervening claims 34 and 35. That is, independent claim 121 recites a method for inserting a digital signature into digital data where the digital data comprises bits and the method comprises: assigning predetermined bits of the digital data for receiving the digital signature; signing the digital data excluding the predetermined bits resulting in the digital signature; inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data; providing time data identifying the time the digital data was created; concatenating the hash and the time data; applying a one-way hashing function to the concatenated hash and time data resulting in a second hash; encrypting the second hash instead of the first hash to result in a time stamp containing the digital signature, wherein both the digital data and the time data are subsequently authenticated; transmitting the hash and signature to a third party for performance of the providing, concatenating, and encrypting steps; and receiving the time stamp from the third party prior to the inserting step; wherein the trusted third party resides at an internet address and the transmitting and receiving steps are done through the internet.

Independent claim 122 is similar in scope to original claim 1 but adds the features of original claim 38 as well as intervening claim 4. That is, independent claim 122 recites a method for inserting a digital signature into digital data where the digital data

comprises bits and the method comprises: assigning predetermined bits of the digital data for receiving the digital signature; inserting associated data into the digital data; signing the digital data excluding the predetermined bits resulting in the digital signature; and inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and associated data; storing an identifier in a memory corresponding to each of at least one user of a device which creates the digital data; recognizing a user of the device whose identifier is stored in the memory; and outputting the identifier corresponding to the recognized user from the memory to be inserted as the associated data. Dependent Claim 123 directly or indirectly depends upon Claim 122.

Independent claim 124 is similar in scope to original claim 47 but adds the features of original claims 50 and 68. That is, claim 124 recites an encoder for inserting a digital signature into digital data where the digital data comprises bits and the encoder comprises: means for assigning predetermined bits of the digital data for receiving the digital signature; means for inserting associated data into the digital data prior to signing the digital data, the associated data comprising at least two fields; means for signing the digital data excluding the predetermined bits resulting in the digital signature; and means for inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and the associated data. Dependent Claims 125 and 126 directly or indirectly depend upon Claim 124.

Independent claim 127 is similar in scope to original claim 47 but adds the features of original claim 72 as well as intervening claims 50, 65, and 71. That is claim 127 recites an encoder for inserting a digital signature into digital data where the digital data

comprises bits and the encoder comprises: means for assigning predetermined bits of the digital data for receiving the digital signature; means for receiving associated data from a Global Positioning Satellite transmission, the associated data comprising data identifying the identity of an owner of the digital data; means for inserting the associated data into the digital data prior to signing the digital data; means for signing the digital data excluding the predetermined bits resulting in the digital signature; and means for inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and the associated data.

Independent claim 128 is similar in scope to original claim 47 but adds the features of original claim 47 but adds the features of original claim 82 as well as intervening claims 50, 80, and 81. That is, claim 128 recites an encoder for inserting a digital signature into digital data where the digital data comprises bits and the encoder comprises: means for assigning predetermined bits of the digital data for receiving the digital signature; means for inserting associated data into the digital data prior to signing the digital data; means for signing the digital data excluding the predetermined bits resulting in the digital signature; means for inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and the associated data; means for providing time data identifying the time the digital data was created; means for concatenating the hash and the time data; means for applying a one-way hashing function to the concatenated hash and time data resulting in a second hash; means for encrypting the second hash instead of the first hash to result in a time stamp containing the digital signature, wherein both the digital data and the time data are subsequently authenticated; means for transmitting the hash to a third

party for providing the time stamp and concatenating the hash and time stamp; and means for receiving the second hash from the third party prior to encryption; wherein the trusted third party resides at an internet address and the means for transmitting and receiving is a computer capable of accessing the internet and receiving the transmitted second hash.

Independent claim 129 is similar in scope to original claims 47 but adds the features of original claims 86 as well as intervening claims 50 and 84. That is, claim 129 recites an encoder for inserting a digital signature into digital data where the digital data comprises bits and the encoder comprises: means for assigning predetermined bits of the digital data for receiving the digital signature; a memory for storing an identifier corresponding to each of at least one user of a device which creates the digital data; recognition means for recognizing a user of the device whose identifier is stored in the memory, wherein the recognition means is a fingerprint recognition system; output means for outputting the identifier corresponding to the recognized user from the memory to be inserted as associated data; means for inserting the associated data into the digital data prior to signing the digital data; means for signing the digital data excluding the predetermined bits resulting in the digital signature; and means for inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and the associated data.

Independent claim 130 is similar in scope to original claim 94 but adds the features of original claim 95. That is, claim 130 recites a method for inserting data into digital data for subsequent authentication of the digital data where the method comprises: receiving data from a radio frequency transmission; inserting the data into the digital data; and authenticating the digital data.

Independent claim 131 is similar in scope to original claim 94 but adds the features of original claim 96. That is, claim 130 recites a method for inserting data into digital data for subsequent authentication of the digital data where the method comprises: receiving data from an internet link; inserting the data into the digital data; and authenticating the digital data.

Independent claim 132 is similar in scope to original claim 98 but adds the features of original claim 99. That is, claim 132 recites a device for inserting data into a digital data for subsequent authentication of the digital data where the device comprises: an antenna for receiving data from a radio frequency transmission; means for inserting the data into the digital image; and means for authenticating the digital data.

Independent claim 133 is similar in scope to original claim 98 but adds the features of original claim 100. That is, claim 133 recites a device for inserting data into a digital image for subsequent authentication of the digital image where the device comprises: a computer capable of accessing the internet and receiving data from an internet link; means for inserting the data into the digital image; and means for authenticating the digital image.

Finally, independent claim 134 is similar in scope to original claim 112 but which adds the features of original claim 114. That is, claim 134 recites a device for inserting data into digital data where the device comprises: a memory for storing an identifier corresponding to each of at least one user of the device; a fingerprint recognition means for recognizing a user of the device whose identifier is stored in the memory; means for outputting the identifier corresponding to the recognized user from the memory; and means for inserting data corresponding to the identifier into the digital data.

Each of the appealed claims, mentioned supra, is set forth in the Appendix.

VIII. THE PRIOR ART RELIED UPON

The references relied upon by the Examiner in rejecting Claims 1-3, 5-16, 18-26, 33-37, 47-49, 51-62, 64-72, and 79-83 are U.S. Patent No. 5,646,997 to Barton and Applied Cryptography by Schneier. The references relied upon by the Examiner in rejecting Claims 27-32 and 73-78 are Barton Schneier, and U.S. Patent No. 5,579,393 to Conner. The references relied upon by the Examiner in rejecting claims 38-41, 84-87, and 106-116 are Barton, Schneier, and U.S. Patent No. 5,771,101 to Bramall. The references relied upon by the Examiner in rejecting claims 117-121, 124-128, and 130-133 are Barton and Schneier. The references relied upon by the Examiner in rejecting claims 122, 123, 129, and 134 are Barton, Schneier, and Bramall.

IX. THE ISSUES

The issues raised in the Final Rejection dated August 14, 2000 remaining for resolution are as follows:

A. Are Claims 1-3, 5-16, 18-26, 33-37, 47-49, 51-62, 64-72, 79-83, 117-121, 124-128, and 130-133 on appeal patentable, under 35 U.S.C. § 103, over the combination of Barton and Schneier?

B. Are Claims 27-32 and 73-78 on appeal patentable, under 35 U.S.C. § 103, over the combination of Barton, Schneier, and Conner?

C. Are Claims 38-41, 84-87, 106-116, 122, 123, 129, and 134 on appeal patentable, under 35 U.S.C. § 103, over the combination of Barton, Schneier, and Bramall?

X. THE REFERENCES

Barton discloses embedding a digital signature of digital data into data by inserting the signature into predetermined bit positions of the digital data and excluding the predetermined bits from the signature. Furthermore, Barton discloses embedding additional data into the digital data. Schneier discloses methods for creating digital signatures using hash functions and a verification method for the signature consisting of decrypting the original hash and comparing it to a re-computed hash. Schneier also discloses time-stamping of the digital document to be authenticated. Conner discloses inserting a digital signature into a header in digital data that is authenticated. Bramall discloses a security system for data handling equipment wherein a preauthorized user of digital image generating equipment is recognized by the equipment.

XI. GROUPING OF THE CLAIMS

The prior art rejections of issue herein apply to more than one claim. Despite this, Appellants submit that the rejected claims stand or fall together.

XII. APPELLANT'S ARGUMENTS

In summary, Appellants submit that the claimed invention is not suggested or rendered obvious to skilled artisans by any proper combination of the prior art of record because:

1. there is no teaching or suggestion in the cited references to place a public key, needed to decrypt the digital signature, into the associated data (claims 17, 22-24, 63, 68-70, 117-119, and 124-126);

2. there is no teaching or suggestion in the cited references to receive associated data from an external source such as from a global positioning satellite transmission (claims 26, 72, 120, and 127), from a radio transmission (claims 95, 99, 130, and 132), or via an Internet link (claims 96, 100, 131, and 133);

3. there is no teaching or suggestion in the cited references of transmitting a hash and signature to a third party over the Internet and receiving a time stamp from the third party over the Internet (claims 36, 82, 121, and 128); and

4. there is no teaching or suggestion in the cited references of recognizing a user of the device whose identifier is stored in memory and inserting the identifier as the associated memory (claim 38, 108, 112, and 122), particularly where the means to recognize the user is a fingerprint recognition means (claims 40, 86, 114, 129, and 134).

A. The rejection of Claims 1-3, 5-16, 18-26, 33-37, 47-49, 51-62, 64-72, 79-83, 117-121, 124-128, and 130-133 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Barton in view of Schneier is improper.

In the Final Rejection dated August 14, 2000, Claims 1-3, 5-16, 18-26, 33-37, 47-49, 51-62, 64-72, 79-83, 117-121, 124-128, and 130-133 of the instant application were rejected under 35 U.S.C. § 103 as being allegedly unpatentable over the combination of Barton and Schneier.

Applicants respectfully submit that the Examiner is using impermissible hindsight in combining the Barton and Schneier references and thus their combination to defeat the patentability of the claims is improper. That is, there is no motivation to combine the watermarking scheme of Barton with the public/private key teaching of Schneier.

To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, **and not based on applicant's disclosure**. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Furthermore, recently the U.S. Court of Appeals for the Federal Circuit (the "Federal Circuit") restated the legal test applicable to rejections under 35 U.S.C. § 103(a) (*In re Rouffet*, 47 USPQ2d 1453 (Fed. Cir., July 15, 1998)). The Court stated:

> [V]irtually all [inventions] are combinations of old elements. Therefore

an Examiner may often find every element of a claimed invention in the prior art. Furthermore, rejecting patents solely by finding prior art corollaries for the claimed elements would permit an Examiner to use the claimed invention itself as a blueprint for piecing together elements in the prior art to defeat the patentability of the claimed invention. Such an approach would be "an illogical and inappropriate process by which to determine patentability." To prevent the use of hind sight based on the invention to defeat patentability of the invention, this court requires the Examiner to show a motivation to combine the references that create the case of obviousness. The Board [of Appeals] did not, however, explain what specific understanding or technological principle within the knowledge of one of ordinary skill in the art would have suggested the combination. Instead, the Board merely invoked the high level of skill in the field of the art. **If such a rote indication could suffice to supply a motivation to combine, the more sophisticated scientific fields would rarely, if ever, experience a patentable technical advance.** Instead, in complex scientific fields, the Board could routinely identify the prior art elements in an application, invoke the lofty level of skill, and rest its case for rejection. To counter this potential weakness in the obviousness construct **the suggestion to combine requirements stands as a critical safeguard against hindsight analysis and rote application of the legal test for obviousness.**

In re Rouffet, 47 USPQ2d 1457-58 (Fed. Cir., July 15, 1998) (citations omitted, emphasis added).

More recently, the Federal Circuit again dealt with what is required to show a motivation to combine references under 35 U.S.C. § 103(a). In this case the court reversed the decision of the Board of appeals stating:

> [R]ather then pointing to specific information in Holiday or Shapiro that suggest the combination..., the Board instead described in detail the similarities between the Holiday and Shapiro references and the claimed invention, noting that one reference or the other-in combination with each other... described all of the limitations of the pending claims. Nowhere does the Board particularly identify any suggestion, teaching, or motivation to combine the ... references, nor does the Board make specific-or even inferential-findings concerning the identification of the relevant art, the level of ordinary skill in the art, the nature of the problem to be solved, or any factual findings that might serve to support a proper obviousness analysis.
>
> *In re Dembiczak*, 50 USPQ2d 1614, 1618 (Fed. Cir., April 28, 1999) (citations omitted).

Thus, from both *In re Rouffet* and *In re Dembiczak* it is clear that the Federal Circuit requires a specific identification of a suggestion, motivation, or teaching why one of ordinary skill in the art would have been motivated to select the references and combine them. This the Examiner has not done. The Examiner only states that it would be obvious "since the signing method disclosed in the applied Schneier reference uses a public/private key signing technique, it would be obvious to include identification of the public key in the field mentioned by Barton so that the recipient/verifier could more easily verify the signature" (see page 3 of the Final Official Action). *In re Rouffet* and *In re Dembiczak* make it clear that this alone is not enough.

The Examiner makes a rote statement about obviousness in the highly technically advanced field of electronic watermarking and makes a statement why the combination would be obvious (to make it more easy to verify the signature) without making any determination of the level of skill in the art at the time of the invention and

the problems facing those in the art at the time of the invention which would make the combination obvious. In fact, the Examiner does not argue that the combination would be obvious to those skilled in the art at the time of the invention, but only that it would be obvious. The Examiner does not make a showing that those in the art at the time of the invention even recognized the problem solved by inserting the public/private key in the associated data. Without such showings, the combination cannot be said to be obvious. **Furthermore, Schneier merely discloses a public/private key signing technique, it has no suggestion or teaching of adding the public/private key to the data to be embedded.**

Furthermore, with regard to features 2-3 above, Applicants respectfully submit that the Examiner is using impermissible hindsight in combining the references with the knowledge of an ordinarily skilled artisan in the art at the time of the invention. Thus, their combination to defeat the patentability of the claims is improper. That is, there is no motivation to combine the watermarking schemes of Barton, Schneier, or Conner with any specific understanding or technological principle within the knowledge of one of ordinary skill in the art regarding:

> receiving associated data from an external source such as from a global positioning satellite transmission, from a radio transmission, or via an Internet link; and
>
> transmitting a hash and signature to a third party over the Internet and receiving a time stamp from the third party over the Internet.

In re Rouffet and *In re Dembiczak* also make it clear that the Federal Circuit requires a specific identification of a suggestion, motivation, or teaching why one of ordinary skill in the art would have been motivated to select the references and combine them with an identification of the level of skill in the art at the time of the invention which would make him likely to combine his skill with the teachings of the art to come up with the invention. This the Examiner has not done. The Examiner merely argues that these features are generally known in the art and that they would be obvious in combination with the watermarking scheme of the present invention without making a showing why it would have been obvious to combine these general features with a watermarking scheme.

Specifically, with regard to feature 2, the Examiner does not cite any references in support of his argument but takes Official Notice that receiving external data by way of GPS and radio and internet transmissions is well known in the art (See page 5 of the Final Official Action). However, the Examiner makes no showing why the combination of these features with a watermarking scheme would be obvious to those of ordinary skill in the art at the time of the invention.

With regard to feature 3, the Examiner also does not cite any references in support of his argument, nor does the Examiner make any showing of the level of skill in the art at the time of the invention, nor of the problems facing those skilled in the art at the time of the invention. Instead, the Examiner lists reasons why feature 3 would be obvious (see page 7, lines 12-22 of the previous Official Action). However, without such a showing, Applicants respectfully submit that these reasons can only be

gleaned from Applicant's disclosure and thus the Examiner has used impermissible hindsight.

Thus, Applicants respectfully submit that the Examiner, without identifying a suggestion, motivation, or teaching for combining the references, has used impermissible hindsight to reject the claims under 35 U.S.C. § 103(a). As discussed above, the Federal Circuit in *In re Rouffet* stated that virtually all inventions are combinations of old elements. Therefore an Examiner may often find every element of a claimed invention in the prior art. To prevent the use of hindsight based on the invention to defeat patentability of the invention, the Examiner is required to show a motivation to combine the references that create the case of obviousness. Applicants respectfully submit that the Examiner has not met this burden.

Thus, Applicants respectfully submit that the Examiner, without identifying the level of skill in the art at the time of the invention or a recognition of the problem addressed by features 1-3 of the present invention (as outlined above), has used impermissible hindsight in making the rejections under 35 U.S.C. § 103(a).

In light of the state of the law as set forth by the Federal Circuit and the Examiner's lack of specificity with regard to the level of skill in the art at the time of the invention, applicants respectfully submit that the rejections for obviousness under 35 U.S.C. § 103(a) lack the requisite motivation and must be withdrawn. Thus, Applicants respectfully submit that independent claims 1, 47, 117, 120, 121, 124, 127, 128, and 130-133 are allowable and dependent claims 2, 3, 5-15, 18-26, 33-37, 48, 49, 51-62, 64-72, 79-83, 118, 119, 125, and 126 are allowable therewith.

B. The rejection of Claims 27-32 and 73-78 on appeal, under 35 U.S.C. § 103, as being allegedly unpatentable over the combination of Barton, Schneier, and Conner, is improper.

In the Final Rejection dated August 14, 2000, Claims 27-32 and 73-78 of the instant application were rejected under 35 U.S.C. § 103 as being allegedly unpatentable over the combination of Barton, Schneier, and Conner.

Appellants respectfully submit that the claims on appeal (27-32 and 73-78) are not obvious from this combination of references in view of the remarks submitted hereinabove and are allowable as depending from an allowable base claim (1 and 47, respectively).

C. The rejection of Claims 38-41, 84-87, 106-116, 122, 123, 129, and 134, on appeal, under 35 U.S.C. § 103, as being allegedly unpatentable over the combination of Barton, Schneier, and Bramall is improper.

In the Final Rejection dated August 14, 2000, Claims 38-41, 84-87, 106-116, 122, 123, 129, and 134 of the instant application were rejected under 35 U.S.C. § 103 as being allegedly unpatentable over the combination of Barton, Schneier, and Bramall. Appellants respectfully submit that claims 38-41, 84-87, 106-116, 122, 123, 129, and 134 on appeal are not obvious from this combination of references in view of the remarks submitted hereinabove.

Furthermore, with regard to feature 4 above, Applicants respectfully submit that the Examiner is using impermissible hindsight in combining the references with the knowledge of an ordinarily skilled artisan in the art at the time of the invention. Thus, their combination to defeat the patentability of the claims is improper. That is,

there is no motivation to combine the watermarking schemes of Barton, Schneier, or Bramall with any specific understanding or technological principle within the knowledge of one of ordinary skill in the art regarding:

> recognizing a user of the device whose identifier is stored in memory and inserting the identifier as the associated memory, particularly where the means to recognize the user is a fingerprint recognition means.

With regard to feature 4, the Examiner again does not cite any references in support of his argument but takes Official Notice that biometric identification, such as fingerprint identification is well known in the art and that it would be obvious to use it to gain its advantages. However, once again, the Examiner makes no showing of the level of skill in the art at the time of the invention nor the problems facing those skilled in the art at the time of the invention. The Examiner merely states that biometric identification has certain advantages, thus it would be obvious to use it. Applicants respectfully submit that the fact that a feature has advantages is not the legal test for obviousness. There must be a motivation in the art at the time of the invention which suggests its combination with another reference. The Examiner has not made any such showing.

Based on the above arguments and remarks, Appellants respectfully submit that the claims of the instant invention on appeal are not obvious over the combination of Barton, Schneier, Conner, and Bramall. Consequently, the rejection of the claims based on the above combination of references is in error.

Thus, Applicants respectfully submit that the Examiner, without identifying the level of skill in the art at the time of the invention or a recognition of the problem addressed by feature 4 of the present invention (as outlined above), has used impermissible hindsight in making the rejections under 35 U.S.C. § 103(a).

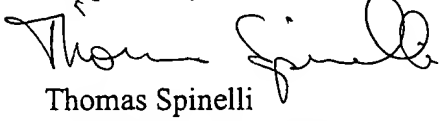
In light of the state of the law as set forth by the Federal Circuit and the Examiner's lack of specificity with regard to the level of skill in the art at the time of the invention, applicants respectfully submit that the rejections for obviousness under 35 U.S.C. § 103(a) lack the requisite motivation and must be withdrawn. Thus, Applicants respectfully submit that independent claims 1, 47, 108, 112, 122, 129 and 134 are allowable and dependent claims 38-41, 84-87, 106, 107, 109-111, 113-116, and 123 are allowable therewith.

XIII. CONCLUSION

In view of the remarks submitted hereinabove, the references applied against Claims 1-3, 5-16,18-41, 47-49, 51-62, 64-87, and 108-134 on appeal do not render those claims unpatentable under 35 U.S.C. § 103. Thus, Appellant submits that the § 103 rejections are in error and must be reversed.

The Commissioner is hereby authorized to charge any additional fees or credit any overpayment in connection herewith to our Deposit Account No. 19-1013. A triplicate copy of this sheet is enclosed.

Respectfully submitted,



Thomas Spinelli
Registration No. 39,533

SCULLY SCOTT MURPHY & PRESSER
400 Garden City Plaza
Garden City, New York 11530
(516) 742-4343

TS/cm

APPENDIX

CLAIMS ON APPEAL:CLAIMS 1-3, 5-16,18-41, 47-49, 51-62, 64-87, and 108-134

Application Serial No. 09/294,956

1. A method for inserting a digital signature into digital data, the digital data comprising bits, the method comprising the steps of:

assigning predetermined bits of the digital data for receiving the digital signature;

inserting associated data into the digital data;

signing the digital data excluding the predetermined bits resulting in the digital signature; and

inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and the associated data;

wherein at least a portion of the associated data comprises data identifying a public key needed to decrypt the digital signature.

2. The method of claim 1, wherein the signing step comprises:

applying a one-way hashing function to the digital data excluding said predetermined bits resulting in a hash; and encrypting the hash.

3. The method of claim 1, wherein the digital data is selected from a group consisting of image data, video data, and audio data.

5. The method of claim 1, wherein the associated data is inserted into the bits of the digital data excluding the predetermined bits.

6. The method of claim 1, wherein the digital data comprises a plurality of samples, each of the samples being defined by a plurality of the bits, from a most significant bit

to a least significant bit, all of the least significant bits defining the plurality of samples comprising a least significant bit plane, wherein the predetermined bits comprise at least a portion of the least significant bit plane.

7. The method of claim 6, wherein the digital data is an image and each sample is an image pixel.

8. The method of claim 6, wherein the digital data is video and each sample is a spatial temporal sample.

9. The method of claim 6, wherein the digital data is audio and each sample is a time sample.

10. The method of claim 6, wherein the associated data is inserted into at least a portion of the remaining least significant bits in the least significant bit plane.

11. The method of claim 1, wherein the digital data comprises a plurality of samples, each of the samples being defined by a plurality of the bits, further comprising the step of transforming the plurality of bits into an alternative representation having at least first and second characteristic components, wherein the predetermined bits comprise the first characteristic component.

12. The method of claim 11, wherein the digital data is an image and each sample is an image pixel.

13. The method of claim 11, wherein the digital data is video and each sample is a spatial temporal sample.

14. The method of claim 11, wherein the digital data is audio and each sample is a time sample.

15. The method of claim 11, wherein the associated data is inserted into at least a portion of the second characteristic component.

16. The method of claim 15, wherein the alternative representation is a frequency domain representation having high and low frequency components, wherein the first characteristic component is a portion of the high frequency component and the second characteristic component is the remaining high frequency component and the low frequency component.

18. The method of claim 1, wherein the associated data comprises data identifying a source of the digital data.

19. The method of claim 1, wherein the associated data comprises data identifying the identity of an owner of the digital data.

20. The method of claim 19, wherein the digital data is an image and the associated data comprises data identifying a photographer of the image.

21. The method of claim 1, wherein a portion of the associated data is encrypted and a remaining portion of the associated data is unencrypted.

22. The method of claim 1, wherein the associated data comprises at least two fields.

23. The method of claim 22, wherein at least one of the fields comprises data identifying a public key needed to decrypt the digital signature.

24. The method of claim 23, wherein at least one other field comprises data identifying the owner of the public key.

25. The method of claim 1, further comprising the step of receiving the associated data from an external source.

26. The method of claim 25, wherein the external source is a Global Positioning Satellite transmission.

27. The method of claim 1, wherein the digital data is compressed using a compression standard resulting in a compressed file, wherein the method further comprises the steps of:

creating a decompressed file prior to the signing step; signing the decompressed file resulting in the digital signature; and

inserting the digital signature into a header in the compressed file instead of inserting the same into the digital data.

28. The method of claim 27, wherein the digital data is an image and the compression standard is JPEG.

29. The method of claim 27, wherein the digital data is video and the compression standard is MPEG.

30. The method of claim 1, wherein the digital data is compressed using a compression standard resulting in a compressed file, wherein the method further comprises the steps of:

creating a decompressed file prior to the signing step;

inserting the associated data into the decompressed file;

signing the decompressed file resulting in the digital signature; and

inserting the digital signature and associated data into a header in the compressed file instead of inserting the same into the digital data.

31. The method of claim 30, wherein the digital data is an image and the compression standard is JPEG.

32. The method of claim 30, wherein the digital data is video and the compression standard is MPEG.

33. The method of claim 1, wherein the digital data comprises a plurality of samples, each of the samples being defined by a plurality of the bits, from a most significant bit to a least significant bit, all of the least significant bits defining the plurality of samples comprising a least significant bit plane, wherein the method further comprises the steps of:

ignoring the least significant bit plane in the digital data;

concatenating the associated data to the digital data having the ignored least significant bit plane prior to the signing step;

performing the signing step to the digital data having concatenated associated data resulting in the digital signature;

wherein the predetermined bits comprise at least a portion of the least significant bit plane and the associated data is inserted into at least a portion of the remaining least significant bits in the least significant bit plane.

34. The method of claim 1, further comprising the steps of:

providing time data identifying the time the digital data was created;

concatenating the hash and the time data;

applying a one-way hashing function to the concatenated hash and time data resulting in a second hash; and

encrypting the second hash instead of the first hash to result in a time stamp containing the digital signature, wherein both the digital data and the time data are subsequently authenticated.

35. The method of claim 34, further comprising the steps of:

transmitting the hash and signature to a third party for performance of the providing, concatenating, and encrypting steps; and

receiving the time stamp from the third party prior to the inserting step.

36. The method of claim 35, wherein the trusted third party resides at an internet address and the transmitting and receiving steps are done through the internet.

37. The method of claim 34, wherein the time stamp is provided by a semiconductor chip having a tamper resistant clock and a tamper resistant time stamping circuit, wherein the clock outputs the time data which together with the digital signature is signed by the circuit to output the time stamp.

38. The method of claim 1, further comprising the steps of:

storing an identifier in a memory corresponding to each of at least one user of a device which creates the digital data;

recognizing a user of the device whose identifier is stored in the memory; and

outputting the identifier corresponding to the recognized user from the memory to be inserted as the associated data.

39. The method of claim 38, further comprising the steps of storing a private key for signing the digital data in the memory corresponding to each user and using the private key for signing the digital data.

40. The method of claim 38, wherein the recognizing step is accomplished by a fingerprint recognition system.

41. The method of claim 38, wherein the identifier is a name of the recognized user.

47. An encoder for inserting a digital signature into digital data, the digital data comprising bits, the encoder comprising:

means for assigning predetermined bits of the digital data for receiving the digital signature;

means for signing the digital data excluding the predetermined bits resulting in the digital signature;

means for inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data; and

means for inserting associated data into the digital data prior to signing the digital data such that the encoder authenticates both the associated data as well as the digital data;

wherein at least a portion of the associated data comprises data identifying a public key needed to decrypt the digital signature.

48. The encoder of claim 47, wherein the means for signing comprises:

means for applying a one-way hashing function to the digital data excluding said predetermined bits resulting in a hash; and

encrypting the hash.

49. The encoder of claim 47, wherein the digital data is selected from a group consisting of image data, video data, and audio data.

51. The encoder of claim 47, wherein the associated data is inserted into the bits of the digital data excluding the predetermined bits.

52. The encoder of claim 47, wherein the digital data comprises a plurality of samples, each of the samples being defined by a plurality of the bits, from a most significant bit to a least significant bit, all of the least significant bits defining the plurality of samples comprising a least significant bit plane, wherein the predetermined bits comprise at least a portion of the least significant bit plane.

53. The encoder of claim 52, wherein the digital data is an image and each sample is an image pixel.

54. The encoder of claim 52, wherein the digital data is video and each sample is a spatial temporal sample.

55. The encoder of claim 52, wherein the digital data is audio and each sample is a time sample.

56. The encoder of claim 52, wherein the associated data is inserted into at least a portion of the remaining least significant bits in the least significant bit plane.

57. The encoder of claim 47, wherein the digital data is an image comprising a plurality of samples, each of the samples being defined by a plurality of the bits, further comprising means for transforming the plurality of bits into an alternative representation having

at least first and second characteristic components, wherein the predetermined bits comprise the first characteristic component.

58. The encoder of claim 57, wherein the digital data is an image and each sample is an image pixel.

59. The encoder of claim 57, wherein the digital data is video and each sample is a spatial temporal sample.

60. The encoder of claim 57, wherein the digital data is audio and each sample is a time sample.

61. The encoder of claim 57, wherein the associated data is inserted into at least a portion of second characteristic component.

62. The encoder of claim 61, wherein the alternative representation is a frequency domain representation having high and low frequency components, wherein the first characteristic component is a portion of the high frequency component and the second characteristic component is the remaining high frequency component and the low frequency component.

64. The encoder of claim 47, wherein the associated data comprises data identifying a source of the digital data.

65. The encoder of claim 47, wherein the associated data comprises data identifying the identity of an owner of the digital data.

66. The encoder of claim 65, wherein the digital data is an image and the associated data comprises data identifying a photographer of the image.

67. The encoder of claim 47, wherein a portion of the associated data is encrypted and a remaining portion of the associated data is unencrypted.

68. The encoder of claim 47, wherein the associated data comprises at least two fields.

69. The encoder of claim 68, wherein at least one of the fields comprises data identifying a public key needed to decrypt the digital signature.

70. The encoder of claim 69, wherein at least one other field comprises data identifying the owner of the public key.

71. The encoder of claim 65, further comprising means for receiving the associated data from an external source.

72. The encoder of claim 71, wherein the external source is a Global Positioning Satellite transmission.

73. The encoder of claim 47, wherein the digital data is compressed using a compression standard resulting in a compressed file, wherein the encoder further comprises:

means for creating a decompressed file prior to signing the digital data;

means for signing the decompressed file resulting in the digital signature; and

means for inserting the digital signature into a header in the compressed file instead of inserting the same into the digital data.

74. The encoder of claim 73, wherein the digital data is an image and the compression standard is JPEG.

75. The encoder of claim 73, wherein the digital data is video and the compression standard is MPEG.

76. The encoder of claim 47, wherein the digital data is compressed using a compression standard resulting in a compressed file, wherein the encoder further comprises:

means for creating a decompressed file prior to signing the digital data;

means for inserting the associated data into the decompressed file;

means for signing the decompressed file with the associated data inserted therein resulting in the digital signature; and

means for inserting the digital signature and associated data into a header in the compressed file instead of inserting the same into the digital data.

77. The encoder of claim 76, wherein the digital data is an image and the compression standard is JPEG.

78. The encoder of claim 76, wherein the digital data is video and the compression standard is MPEG.

79. The encoder of claim 47, wherein the digital data comprises a plurality of samples, each of the samples being defined by a plurality of the bits, from a most significant bit to a least significant bit, all of the least significant bits defining the plurality of samples comprising a least significant bit plane, wherein the encoder further comprises:

means for ignoring at least a portion of the least significant bit plane in the digital data;

means for concatenating the associated data to the digital data having the ignored least significant bit plane prior to signing the digital data;

means for signing the digital data having the concatenated associated data resulting in the digital signature;

wherein the predetermined bits comprise at least a portion of the least significant bit plane and the associated data is inserted into at least a portion of the remaining least significant bits in the least significant bit plane.

80. The encoder of claim 47, further comprising:

means for providing time data identifying the time the digital data was created;

means for concatenating the hash and the time data;

means for applying a one-way hashing function to the concatenated hash and time data resulting in a second hash; and

means for encrypting the second hash instead of the first hash to result in a time stamp containing the digital signature, wherein both the digital data and the time data are subsequently authenticated.

81. The encoder of claim 80, further comprising:

means for transmitting the hash to a third party for providing the time stamp and concatenating the hash and time stamp; and

means for receiving the second hash from the third party prior to encryption.

82. The encoder of claim 81, wherein the trusted third party resides at an internet address and the means for transmitting and receiving is a computer capable of accessing the internet and receiving the transmitted second hash.

83. The encoder of claim 80, further comprising a semiconductor chip having a tamper resistant clock and a tamper resistant time stamping circuit, wherein the clock outputs the

time data which together with the digital signature is signed by the circuit to output the time stamp.

84. The encoder of claim 47, further comprising:

a memory for storing an identifier corresponding to each of at least one user of a device which creates the digital data;

recognition means for recognizing a user of the device whose identifier is stored in the memory; and

output means for outputting the identifier corresponding to the recognized user from the memory to be inserted as the associated data.

85. The encoder of claim 84, wherein a private key for signing the digital data is also stored in memory corresponding to each user, wherein the identifier is inserted as associated data and the private key is used to sign the digital data.

86. The encoder of claim 84, wherein the recognition means is a fingerprint recognition system.

87. The encoder of claim 86, wherein the identifier is a name of the recognized user.

108. (Amended) A method for inserting data into digital data, the method comprising the steps of:

storing an identifier corresponding to each of at least one user of a device which creates the digital data;

recognizing a user of the device whose identifier is stored in the memory;

outputting the identifier corresponding to the recognized user from the memory; and

inserting data corresponding to the identifier into the digital data.

109. The method of claim 108, wherein the inserted data is used for authenticating the digital data.

110. The method of claim 108, wherein the inserted data is used for authenticating information associated with the digital data.

111. The method of claim 108, wherein the identifier is a name of the recognized user.

112. A device for inserting data into digital data, the device comprising:

a memory for storing an identifier corresponding to each of at least one user of the device;

recognition means for recognizing a user of the device whose identifier is stored in the memory;

means for outputting the identifier corresponding to the recognized user from the memory; and

means for inserting data corresponding to the identifier into the digital data.

113. The device of claim 112, wherein a private key for signing the digital data is also stored in memory corresponding to each user, wherein the identifier is inserted into the digital data and the private key is used to subsequently sign the digital data.

114. The device of claim 112, wherein the recognition means is a fingerprint recognition means.

115. The device of claim 112, wherein the device is a digital image generation device and the digital data represents an image.

116. The device of claim 112, wherein the image generation device is selected from a group consisting of a digital camera, a digital video camera, and a digital scanner.

117. A method for inserting a digital signature into digital data, the digital data comprising bits, the method comprising the steps of:

assigning predetermined bits of the digital data for receiving the digital signature;

inserting associated data into the digital data;

signing the digital data excluding the predetermined bits resulting in the digital signature; and

inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and associated data;

wherein the associated data comprises at least two fields.

118. The method of claim 117, wherein at least one of the fields comprises data identifying a public key needed to decrypt the digital signature.

119. The method of claim 118, wherein at least one other field comprises data identifying the owner of the public key.

120. A method for inserting a digital signature into digital data, the digital data comprising bits, the method comprising the steps of:

assigning predetermined bits of the digital data for receiving the digital signature;

receiving associated data from a Global Positioning Satellite transmission;

inserting the associated data into the digital data;

signing the digital data excluding the predetermined bits resulting in the digital signature; and

inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and associated data.

121. A method for inserting a digital signature into digital data, the digital data comprising bits, the method comprising the steps of:

assigning predetermined bits of the digital data for receiving the digital signature;

signing the digital data excluding the predetermined bits resulting in the digital signature;

inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data;

providing time data identifying the time the digital data was created;

concatenating the hash and the time data;

applying a one-way hashing function to the concatenated hash and time data resulting in a second hash;

encrypting the second hash instead of the first hash to result in a time stamp containing the digital signature, wherein both the digital data and the time data are subsequently authenticated;

transmitting the hash and signature to a third party for performance of the providing, concatenating, and encrypting steps; and

receiving the time stamp from the third party prior to the inserting step;

wherein the trusted third party resides at an internet address and the transmitting and receiving steps are done through the internet.

122. A method for inserting a digital signature into digital data, the digital data comprising bits, the method comprising the steps of:

assigning predetermined bits of the digital data for receiving the digital signature;

inserting associated data into the digital data;

signing the digital data excluding the predetermined bits resulting in the digital signature; and

inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and associated data;

storing an identifier in a memory corresponding to each of at least one user of a device which creates the digital data;

recognizing a user of the device whose identifier is stored in the memory; and

utputting the identifier corresponding to the recognized user from the memory to be inserted as the associated data.

123. The method of claim 122, wherein the recognizing step is accomplished by a fingerprint recognition system.

124. An encoder for inserting a digital signature into digital data, the digital data comprising bits, the encoder comprising:

means for assigning predetermined bits of the digital data for receiving the digital signature;

means for inserting associated data into the digital data prior to signing the digital data, the associated data comprising at least two fields;

means for signing the digital data excluding the predetermined bits resulting in the digital signature; and

means for inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and the associated data.

125. The encoder of claim 124, wherein at least one of the fields comprises data identifying a public key needed to decrypt the digital signature.

126. The encoder of claim 125, wherein at least one other field comprises data identifying the owner of the public key.

127. An encoder for inserting a digital signature into digital data, the digital data comprising bits, the encoder comprising:

means for assigning predetermined bits of the digital data for receiving the digital signature;

means for receiving associated data from a Global Positioning Satellite transmission, the associated data comprising data identifying the identity of an owner of the digital data;

means for inserting the associated data into the digital data prior to signing the digital data;

means for signing the digital data excluding the predetermined bits resulting in the digital signature; and

means for inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and the associated data.

128. An encoder for inserting a digital signature into digital data, the digital data comprising bits, the encoder comprising:

means for assigning predetermined bits of the digital data for receiving the digital signature;

means for inserting associated data into the digital data prior to signing the digital data;

means for signing the digital data excluding the predetermined bits resulting in the digital signature;

means for inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and the associated data;

means for providing time data identifying the time the digital data was created;

means for concatenating the hash and the time data;

means for applying a one-way hashing function to the concatenated hash and time data resulting in a second hash;

means for encrypting the second hash instead of the first hash to result in a time stamp containing the digital signature, wherein both the digital data and the time data are subsequently authenticated;

means for transmitting the hash to a third party for providing the time stamp and concatenating the hash and time stamp; and

means for receiving the second hash from the third party prior to encryption;

wherein the trusted third party resides at an internet address and the means for transmitting and receiving is a computer capable of accessing the internet and receiving the transmitted second hash.

129. An encoder for inserting a digital signature into digital data, the digital data comprising bits, the encoder comprising:

means for assigning predetermined bits of the digital data for receiving the digital signature;

a memory for storing an identifier corresponding to each of at least one user of a device which creates the digital data;

recognition means for recognizing a user of the device whose identifier is stored in the memory, wherein the recognition means is a fingerprint recognition system;

output means for outputting the identifier corresponding to the recognized user from the memory to be inserted as associated data

means for inserting the associated data into the digital data prior to signing the digital data;

means for signing the digital data excluding the predetermined bits resulting in the digital signature; and

means for inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and the associated data;

130. A method for inserting data into digital data for subsequent authentication of the digital data, the method comprising the steps of:

receiving data from a radio frequency transmission;

inserting the data into the digital data; and

authenticating the digital data.

131. A method for inserting data into digital data for subsequent authentication of the digital data, the method comprising the steps of:

receiving data from an internet link;

inserting the data into the digital data; and

authenticating the digital data.

132. A device for inserting data into a digital data for subsequent authentication of the digital data, the device comprising:

an antenna for receiving data from a radio frequency transmission;

means for inserting the data into the digital image; and

means for authenticating the digital data.

133. A device for inserting data into a digital image for subsequent authentication of the digital image, the device comprising:

a computer capable of accessing the internet and receiving data from an internet link;

means for inserting the data into the digital image; and

means for authenticating the digital image.

134. A device for inserting data into digital data, the device comprising:

a memory for storing an identifier corresponding to each of at least one user of the device;

a fingerprint recognition means for recognizing a user of the device whose identifier is stored in the memory;

means for outputting the identifier corresponding to the recognized user from the memory; and

means for inserting data corresponding to the identifier into the digital data.